FOR508

Advanced Incident Response, Threat Hunting, and Digital Forensics

FOR508 is the most complete incident response and threat hunting course on the market. It teaches the advanced skills to hunt down, identify, counter, and recover from a wide range of threats within enterprise networks, including APT nation-state adversaries, financial crime syndicates, and ransomware operators. An emphasis on developing analytical skills and anomaly detection is in the DNA of the course, ensuring that learned skills are transferable to any network and any security tool stack.

Cybersecurity statistics indicate that there are 2,200 cyber attacks per day, with a cyber attack happening every 39 seconds on average. In the US, a data breach costs an average of $9.44M, and cybercrime is predicted to cost $8 trillion by the end of 2023.

Source: eSentire 2022 Official Cybercrime Report

Fall 2023 Update

A complete replacement of every lab exercise provides a foundation of 50% new course content. A trove of forensic data representing the latest attack techniques allows attendees to master the tools, techniques, and procedures necessary to effectively hunt, detect, and contain a variety of adversaries.

NEW CONTENT

- Introducing a brand-new attack scenario -- students investigate a real network hacked by a professional red team emulating real-world adversaries using attack techniques currently in the wild.
- Attendees gain experience finding a wide variety of attack patterns, including advanced credential theft, multiple types of malware persistence, and forensic artifacts left behind by PowerShell, WMI, Cobalt Strike, Sliver, Impacket, Covenant, RMM tools, and much more.
- The Hunting Across the Enterprise section was re-imagined and now includes multiple opportunities for hands-on experience with the Velociraptor incident response platform.
- Memory Forensics is now at the state of the art with exciting new techniques to leverage YARA signatures to detect advanced malware hiding techniques, a new capability to extract cached files from memory, and more insight into investigating loaded vulnerable drivers (BYOVD).

UPDATED FEATURES

- Many courseware updates were made to support the new hands-on exercise data set.
- An entire day of advanced forensic techniques provides the means to counter current anti-forensic activities and perform critical data recovery.
- The malware persistence and DLL hijack section was updated to reflect new tools and techniques
- Event log analysis was updated with the latest changes to PowerShell logging, including PowerShell Core versions, and a new section on Windows Defender logs, Detection History, and MPLogs.
- Major updates and capabilities were added to the forensic timelining section, including additions like PowerShell transcripts and Windows Server User Access Logs (UAL).

NEW LABS

- Every hands-on lab is completely new!
- Forensic and threat hunting techniques are used to identify the entire attack cycle, identifying initial reconnaissance, exploit weaponization and delivery, attacker persistence, and post-exploitation behavior.
- Solving the final intrusion lab requires investigating artifacts on over thirty systems including Windows 10 and 11 workstations, DMZ servers, a domain controller, internal development servers, and hosted Exchange email.
- Use memory forensics to find a wide variety of advanced malware, including Cobalt Strike, Meterpreter, Amadey, Emotet, Solar Marker, custom nation state backdoors, rootkits, and bootkits
- Bonus labs and materials ensure students can continue practicing long after the course is completed.

The average data breach lifecycle is 277 days—meaning it takes that long for organizations to identify and contain an active breach.

Source: IBM Cost of Data Breach Report

"*FOR508 exceeded my expectations in every way. It provided me the skills, knowledge, and tools to effectively respond to and handle APTs and other enterprise-wide threats*"

– Josh M., US Federal Agency

GIAC Certified Forensic Analyst (GCFA)

For more information: sans.org/FOR508

SANS | GIAC CERTIFICATIONS